IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Jamal Benbrahim	Attorney Docket No.: IGT1P376/P-227
Application No.: 09/880,474	Examiner: Emmanuel Omotosho
Filed: June 12, 2001	Group: 3714
Title: METHOD AND APPARATUS FOR SECURING GAMING MACHINE OPERATING DATA	Confirmation No.: 5212

CERTIFICATE OF EFS-WEB TRANSMISSION
I hereby certify that this correspondence is being transmitted electronically through EFS-WEB to the Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450 on June 8, 2007.

Signed: /swx/
Susan W. Xu

APPLICANT INITIATED INTERVIEW REQUEST FORM

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Tentative Participants:

1) Ray Mahboubian
2)
3)
4)

Proposed Date of Interview: **June 13, 2007**

Proposed Time: **2:00 PM (Eastern Time)**

Type of Interview Requested:

☒ Telephone ☐ Personal ☐ Video Conference

Exhibit to be Shown or Demonstrated: ☐ Yes ☐ No
If yes, provide brief description:

ISSUES TO BE DISCUSSED

Issues (Rej., Obj., etc.)	Claims/ Fig., #s	Prior Art	Discussed	Agreed	Not Agreed
1) 103	Claim 18	*Graunke et al*	☐	☐	☐
2)			☐	☐	☐
3)			☐	☐	☐

BRIEF DESCRIPTION OF AGRUMENTS TO BE PRESENTED:

It is respectfully submitted that the Examiner's rejection is improper for failing to address all of the recited features of the claimed invention. More particularly, it is respectfully submitted that the Examiner has not even addressed the claim feature of: sending information relating to the decrypted one of the first or second operating data to a remote device to be authenticated by the remote device (claim 18). Instead, the Examiner has merely alleged that *Graunke et al.* teaches a manner of encryption suitable for the distribution of software without addressing this claimed feature (Final Office Action, page 3). Accordingly, it is respectfully submitted that the Examiner's rejection should be withdrawn. Moreover, it is respectfully submitted that *Graunke et al.* does not teach or suggest this claimed feature. This distinction is believed to be apparent as *Graunke et al.* does not teach authentication of decrypted data. Instead, *Graunke et al.* teaches secure distribution of a private key to a user's application program with conditional access based on certification of the trusted player's integrity and authenticity (*Graunke et al.,* Abstract). It should be noted that "once validated, the trusted player uses the private key to decrypt encrypted digital content" (*Graunke et al.,* Abstract). As such, *Graunke et al.* clearly teaches verification of a trusted player before decryption of encrypted digital content, not authentication of decrypted content. In fact, *Graunke et al.* teaches away from the claimed feature of sending information relating to the decrypted one of the first or second operating data to a remote device for authentication by the remote device. Claim 18 and other independent claims recite this feature and are therefore patentable over *Graunke et al.*

Furthermore, it is respectfully submitted that *Graunke et al.* does not teach or suggest taking remedial action when the decrypted one of the first or second set of operating data is not authenticated by the gaming machine. In the Final Office Action, the Examiner has asserted that operations 118, 119, 120, 128 and 138 depicted in Figure 4B of *Graunke et al.* teach this feature (Final Office Action, page 3).

It is noted that *Graunke et al.* describes checking the integrity and authenticity of a trusted player (119) and generate a fail condition (128) if the trusted player is not ok (*Graunke et al.,* Figure 4B). However, contrary to the Examiner's assertion, it is

respectfully submitted that *Graunke et al.* does not teach taking remedial action when the decrypted data is not authenticated by the remote device.

Still further, it is respectfully submitted that *Graunke et al.* does not teach or suggest: (a) taking remedial action including not allowing the decrypted one of the first or second set of operating data to be executed by the gaming machine, (b) storing the decrypted one of the first or second set of operating data when the decrypted one is authenticated by the remote device, and (c) executing the first or second game utilizing the decrypted one of the first or second set of operating data when the decrypted one is authenticated. Accordingly, it is respectfully submitted that claim 1 is patentable over *Graunke et al.* for these additional reasons.

Finally, it is respectfully submitted that the Examiner has failed to establish a prima facie case of obviousness because the Examiner has failed to provide a motivation or suggestion for combining *Rowe* and *Graunke et al.* Instead, the Examiner has merely asserted that "one of ordinary skill in the art would have been forced to seek outside references, such as the *Graunke et al.* reference for disclosure as to the known manners and/or procedures of enacting the encryption as described in the first invention of Rowe" (Final Office Action, page 3).

An interview was conducted on the above-identified application on .

*Note: This form should be completed be applicant and submitted to the examiner in advance of the interview (see MPEP §713.01). This application will not be delay from issue because of applicant's failure to submit a written record of this interview. Therefore, applicant is advised to file a statement of the substance of this interview (37 CFT 1.33(b)) as soon as possible.

(Applicant/Applicant's Representative) Signature)	(Examiner/SPE Signature)

18 (Currently Amended) A method of operating a gaming device, the method comprising:

providing on the gaming device executable code for a plurality of games including a first game and a second game, each of the plurality of games stored in an encrypted format, wherein the plurality of games comprise at least a first set of operating data for the first game comprising at least one of first audio data or first video data for generating the first game on the gaming device, and wherein the first set of operating data is encrypted with a first private key and storing a second set of operating data for the second game comprising at least one of second audio or second video data for generating the second game on the gaming device, wherein the second set of operating data is encrypted with a second private key;

providing the gaming device with only one of the first private key or the second private key to prevent execution of the first game or the second game on the gaming device;

decrypting one of the first set of operating data or the second set of operating data according to the one of the first private key or the second private key selected to recover the one of the first set of operating data or the second set of operating data;

sending information relating to the decrypted one of the first set of operating data or the second set of operating data to a remote device for authentication of ~~to authenticate~~ the decrypted one of the first set of operating data or the second set of operating data; ~~wherein~~

taking remedial action by the gaming device ~~is operable to take remedial action~~ when the decrypted one of first set of operating data or the second set of operating data is not authenticated by the remote device, wherein the remedial action includes not allowing the decrypted one of first set of operating data or the second set of operating data to be executed by the gaming device;

storing the decrypted one of the first set of operating data or the second set of operating data when the decrypted one is authenticated by the remote device; and

~~receiving an element of value for use as credit on the gaming device;~~

~~receiving a bet on an outcome to the first game or the second game using the credit;~~

~~generating~~ executing the first game or the second game on the gaming device utilizing the decrypted one of the first set of operating data or the second set of operating data when the decrypted one is authenticated by the remote device.